Citation 2

SEのための実践情報誌

# 日経オープンシステム

NIKKEI OPEN SYSTEMS

2000 1
January

受入
平成
12.1.14
(財)ソフトウェア
情報センター

特集 ▶p.116

## 21世紀のシステム・エンジニアリング

製品・技術に振り回されず変化に強いシステムを手にする



注目技術 活用のポイント ▶p.188

## あなたはWindows 2000を導入すべきか

注目製品 選択のポイント ▶p.198

## Webアプリケーション・サーバー

BEST AVAILABLE COPY

Open Report

Citation 2

# 解説●リアルタイム監視を行う不正アクセス検出ツール

## 分散配置やメール監視，「仮想おとりマシン」構築機能など機能向上が進む

**不正アクセスをリアルタイムに検出するツールの機能が向上している。メールやWWWアクセスの内容を監視したり，クライアントに配置して漏れなく監視する機能，「おとり」の仮想マシンを作りクラッカをおびきよせる機能を持つ製品などが出てきた。**

不正アクセスをリアルタイムに検出する「IDS (Intrusion Detection System)」と呼ばれるツールの機能向上がめざましい。サーバーのログやネットワークを監視するタイプに加え，クライアントにも配置することを想定したタイプの製品が出てきた。本番稼働中のマシンの中に「おとり」となる仮想マシンを構築し，クラッカをおびきよせその行動を記録する製品も現れた(表1)。

### 診断からリアルタイム監視へ

不正アクセス対策ツールとしては，疑似アタックをかけてセキュリティ・ホールや不適切なシステム設定を診断するタイプの製品の出荷数が多かったが，ここへきて「リアルタイムに検出するIDSを導入するユーザーが診断ツールと同程度に増えてきた」(ラック不正アクセス対策事業本部 ISS &Shakoプロダクトチームリーダー ネットワークセキュリティ コンサルタント 上原孝之氏)。診断後の監視の手段として，検出ツールの導入が広がってきている。

また，不正アクセスは社内から行われるケースも多い。監視ツールにはどのようなアクセスを検出するかをユーザーが定義できるものもある。異常なアクセス，例えば「大量データのダウンロード」や「通常行われないアクセス(例えば，システム部以外からのtelnet)」などを監視するように設定することで，社内不正アクセス対策としても使用できる。

### ログなどを監視

不正アクセスを検出する方法は大き

表1●日本で販売されている不正アクセス検出ツール

| 製品名 | Cisco NetRanger | CyberCop Monitor, CyberCop Sting | HP OpenView Node Sentry | NetProwler (NP), Intruder Alert (ITA) |
|---|---|---|---|---|
| 開発元 | 米Cisco Systems | 米Network Associates | 米Hewlett-Packard | 米AXENT Technologies |
| 日本での販売元 | 日本シスコシステムズ (http://www.cisco.com/jp/)，ヒューコム (http://www-hucom.co.jp/)など | ネットワークアソシエイツ (http://www.nai.com/japan/) | 日本ヒューレット・パッカード (http://www.jpn.hp.com/) | アクセント・テクノロジーズ (http://www.axent.com/)，日新電機 (http://www.elnis.com/fcontents.html) |
| 分類 | ネットワーク監視 | 送受信パケット監視+ホスト監視 | ネットワーク監視 | ネットワーク監視(NP)，ホスト監視(ITA) |
| 稼働するOS | x86 Solaris | Windows NT | Windows NT(エージェント)，Windows NTまたはHP-UX(マネジャ) | Windows NT(NPおよびITAマネジャ)，NT，Solaris，HP-UX，AIX，IRIXなど(ITAエージェント) |
| 価格 | ハード+ソフトで247万2000円から。年間サポート45万円。価格はヒューコムによる | StingはMonitorに付属。標準年間ライセンス1ノードあたり3900円(101ノード以上の場合) | 管理マネジャ，エージェント，それぞれ使用権100万円から | NP+ITA(1マネジャ，1エージェント)で110万円。ITAのマネジャは50万円，エージェントはUNIX版が75万円，NT Server版が24万円，NT Workstation版が2万円 |
| 販売形態 | ラック・マウント型ハードウエア+ソフトウエア。管理コンソール・ソフトウエアとしてOpenView Network Node Managerが別途必要 | ソフトウエア | ソフトウエア。Cisco NetRangerソフトウエアのWindows NT版のOEM。管理コンソールとしてOpenView Network Node Managerが別途必要 | ソフトウエア |



BEST AVAILABLE COPY

Citation 2



*1
このような攻撃パターンをシグネチャと呼ぶ。各ベンダーは100以上のアタックに対応するシグネチャを用意している。新しいセキュリティ・ホールが発見されるとシグネチャの更新が必要になる。

[swatch]
Perlで記述されたログ監視ツール。管理者が指定したアクセスのパターンを検出するとメールなどで警告を発するように設定できる。通常シグネチャによらずログインの失敗などを監視するなどに使用する。

[DoS]
システムやサービスを停止する攻撃。SYN Flood(コネクション開始要求パケットだけを大量に送信する)，TearDrop(分解して送信したパケットのオフセット値を不正にしてパケットの再構築を不能にする)などが有名。

く分けて3つある。1つは，監視対象となるマシン上で動作し，ログなどを監視するもの。ログに，アタックの時に使用されるコマンドのパターンなど特定の文字列が含まれていると不正アクセスとみなす，などの方法をとる*1。

UNIXを対象にしたオープン・ソース・ソフトウエアのswatch*が原理的にはこのタイプだ。欠点は，OSのバグなどを突いてシステムの機能を停止させるDoS (Denial of Service)*攻撃をほとんど防げないことだ。

純粋なホスト監視型だけを提供するベンダーは少なく，以下に述べるいずれかの方式と組み合わせている。

## 流れるパケットを監視

2つめは，ネットワークを監視するもので，監視対象のネットワーク・セグメントを流れるすべてのパケットを取り込み，パケットに含まれるアタックのパターンを探す。

このようなネットワーク監視型では，監視していることをクラッカに検知されないように，IPアドレスを振らずにネットワークにつなぐ。「ステルス・モード」などと呼ばれる。ただし，このままではほかのマシンと通信できないので，もう1枚のネットワーク・インタフェース・カードを装着し，こちらにはIPアドレスを与えて，社内など安全と思われるセグメントに

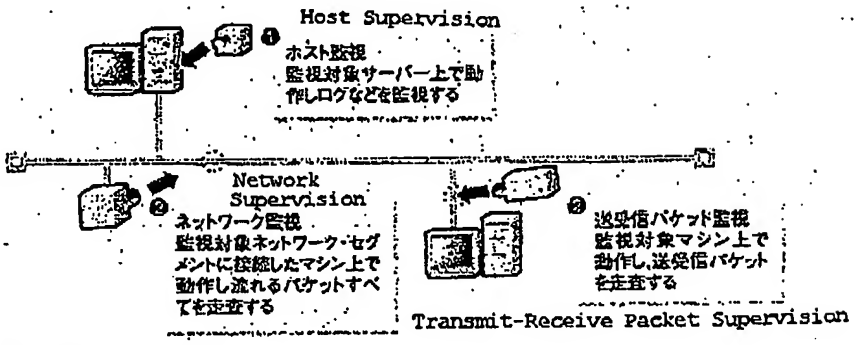


図1●不正アクセス監視ツールの原理
FIB. 1 Principle of Corrupt Access Supervisory Tool

| RealSecure Network Engine (RNE), RealSecure System Agent (RSA) | SecureDetector | Session Wall-3 | エンタープライズICEpac |
|---|---|---|---|
| 米Internet Security Systems | 米ODN Networks | 米Computer Associates | 米NetworkICE |
| アイ・エス・エス (http://www.isskk.co.jp/) | 日本NCR (http://www.ncr.co.jp/)，アクトンテクノロジ (http://www.accton.co.jp/) | アズジェント (http://www.asgent.co.jp/)，ブォーバルクリエイティブ (http://www.forval-c.co.jp/)，オービックビジネスコンサルタント (http://www.obc.co.jp/) | 東陽テクニカ (http://www.toyo.co.jp/) |
| ネットワーク監視(RNE)，ホスト監視(RSA) | ネットワーク監視 | ネットワーク監視 | 送受信パケット監視，ネットワーク監視 |
| Windows NT，Solarisなど | Windows NT | Windows NT/95/98 | Windows NT/95/98 |
| RNEが1デバイス・パック107万8000円から，RSAが1デバイス・パック19万4000円から | ハード+ソフトで1165万円(10セグメント監視ライセンス含む)。価格は日本NCRによる | 34万4000円(25ユーザー，初年度サポート含む)から。価格はアズジェントによる | 年間ライセンス(サポート含む)1ノードあたり7970円(126～250ノードの場合) |
| ソフトウエア | ラック・マウント型ハードウエア+イーサネット・スイッチ(10ポート)+ソフトウエア(米ISSのReal Secure Network Engine) | ソフトウエア | ソフトウエア，別途Microsoft SQL Serverが必要 |

BEST AVAILABLE COPY

Citation 2

*2
検出ツールが稼働するマシンにはIPアドレスがないので、この場合アタックされているマシンのIPアドレスを送信元アドレスとして使いパケットを送る。

*3
同じIPアドレスで、間違ったMACアドレスを持つパケットを混ぜて送ることで、検知ツールをかく乱する手口も紹介されている。MACアドレスが違うパケットは受信側では受け取られない。一方、検知ツールはIPアドレスで見ているため、MACアドレスの違うパケットも含めてパターンを検出する。そのため攻撃を見逃してしまう。

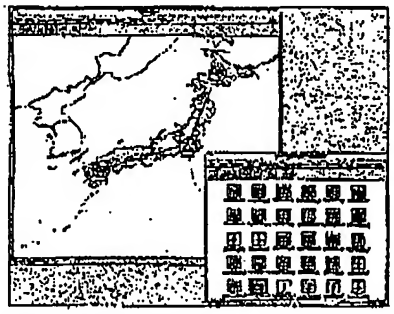

写真1●Cisco NetRanger
ネットワーク監視型。ハードウエアとセットで販売されている。HP OpenView上で監視、操作する。HP OpenView Node SentryはNetRangerソフトウエアのNT版のOEM製品

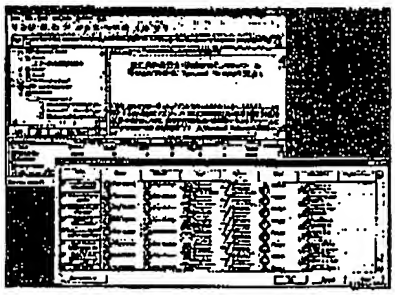

写真2●Session Wall-3
ネットワーク監視型で、不正アクセスのほか、ネットを流れるWWWページやメールを監視し、ルールに触れるページやメールを保存する(背後のウインドウ)。手前のウインドウは監視ルールを定義している

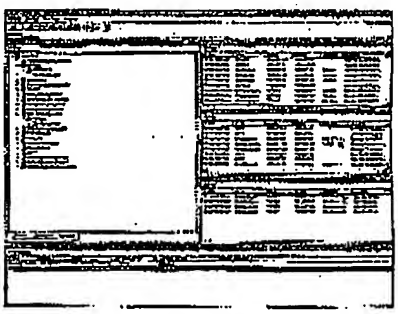

写真3● RealSecure Network Engine (RNE), RealSecure System Agent (RSA)
RNEはネットワーク監視型、RSAはホスト監視型で複数のマシンを集中監視する。SecureDetectorはRealSecureを組み込んだハードウエア

つなぎ，監視・設定を行う。

不正アクセスを検出すると，クラッカにリセット・パケットを送り，コネクションを強制的に切断する機能も，ほとんどの製品が備える[*4]。ファイアウオールに通知しアクセスを遮断する機能やSNMPマネジャにアラートを上げる機能を持つ製品も多い。

## 送受信パケットを監視

3つめは，監視対象マシンの送受信パケットを監視する方法である。ネットワーク監視型では，スイッチなどが介在すると，セグメントの全パケットは監視できない。またトラフィックが高くなると，パケットを取りこぼす可能性もある。そのため，監視対象のマシンすべてにインストールし，そのマシンあてのパケットを見る[*5]。

複数のマシンにインストールするため，監視やアップデートが1台のマシンからできるような集中管理ツールを備えている。デメリットは検出のためのオーバーヘッドにより，性能に影響を与えることだ。オーバーヘッドが許容範囲かどうかは，マシンの性能や用途によるだろう。

## OpenViewやルーターと連動

個々の製品の特徴を見ていこう。

Cisco NetRangerはネットワーク監視型のツールだ(写真1)。x86 Solarisを搭載したラック・マウント型ハードウエアに組み込まれて販売されている。Cisco製のルーターと連携することが特徴だ。不正アクセスを検出すると，ルーターに通知し，クラッカからのアクセスをフィルタリングし遮断してしまう。HP OpenView上で監視，操作するため，別途HP OpenView Network Node Managerが必要になる。

ソフトウエアのみで購入する方法もある。日本ヒューレット・パッカードが販売しているHP OpenView Node Sentryは，Windows NT版NetRangerのOEM製品である。

Session Wall-3もネットワーク監視型だが，アタック検出だけでなく，ネットワークを流れるWWW (World-Wide Web) ページやメールのパケットも監視し，検知ルールに抵触するものは保存する。この機能により，内部における不正アクセスを検知できる。

写真2の手前のウインドウは監視ルールを定義しているウインドウで，パケットの送信元やあて先，含まれる文字列などを設定し，不正と判断するアクセスおよびメール，WWWアクセスを定義する。背後のウインドウは記録したHTML (HyperText Transfer Language) を表示している。

## 複数方式を組み合わせる

複数の方式を組み合わせることを推奨するベンダーもある。セキュリティ・ホール診断ソフトの代表的ツール

BEST AVAILABLE COPY

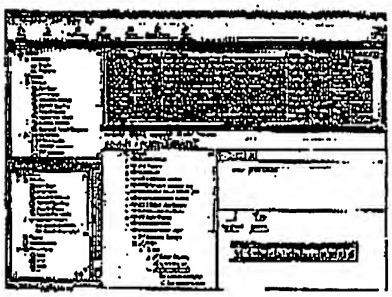

写真4●NetProwler(背後)とIntruder Alert(手前)
NetProwlerはネットワーク監視型で，ホスト監視型のIntruder Alertが1ライセンスが付属している

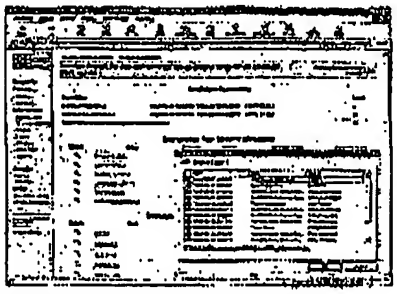

写真5●エンタープライズICEpac
パケット監視型とネットワーク監視型ツールからなる。クライアントに置くことも想定している。背後はレポート，手前は警告ウインドウ

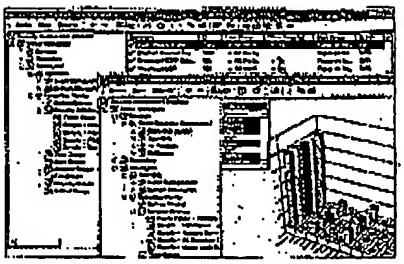

写真6●CyberCop Monitor
受信パケット監視とホスト監視の複合型。書き換えられたページを即座に復元する，などが可能。仮想おとりマシンを構築してクラッカをおびき寄せるCyberCop Stingが付属

Internet Scannerの開発元である米Internet Security Systemsは，ネットワーク監視型のRealSecure Network Engine(RNE)，ホスト監視型のRealSecure System Agentの2製品を販売している。1つのコンソールから両方のツールを使い複数のマシンを集中監視できる(写真3)。検知ルールを定義する機能も備えている。

また日本NCRなどが販売するSecureDetectorは，RNEにハードウエアとスイッチを組み合わせたものだ。

ネット監視ツールにホスト監視ツールを付けて販売しているベンダーもある。NetProwlerはネットワーク監視型で，ホスト監視型であるIntruder Alertの1ライセンスが付属している(写真4)。ルール定義も可能だ。

## クライアントへの配置を想定

エンタープライズICEpaqはネットワーク監視型のBlackICE Sentryと，送受信パケットを監視するBlackICE Proで構成する。BlackICE Proはクライアントにもインストールすることを想定している。分散したBlackICE Proを集中監視，アップデートするためのツールが付属している。

CyberCop Monitorはパケット監視とホスト監視の複合型で，やはりクライアントにもインストールすることを想定し，集中管理機能を持つ。

「このディレクトリは夜間書き換えない」といった設定も可能だ。クラッカにホームページを書き換えられてもバックアップから即座に復元して被害を最小限にとどめる機能を持つ。

CyberCop Monitorに付属するCyberCop Stingは，おとりネットワークを仮想的に作る，というユニークな発想のツールだ。CyberCop Stingが動作するマシンに，本来のIPアドレスのほか複数のアドレスを割り当てておく。それぞれのIPアドレスに米Sun MicrosystemsのマシンやCiscoのルーターのふりをするように指示しておくと，アクセスに対しあたかもSolarisやIOS(Cisco製ルーターのOS)であるように反応する。telnetなどクラッカが狙ってくるサービスをエミュレートしており，その行動を見ていればアクセスが不正な意図を持っているかどうかわかる。

## 使いこなす知識は必要

残念ながら現時点では，IDSを導入しさえすれば万全という訳にはいかない。例えばアクセスの中には明らかな攻撃もあるが，グレー・ゾーンのものもある。その判断には知識が必要だ。

また，検出ルールをユーザーが設定できるタイプでは，GUIにより操作は簡単とはいえ，"予口"を知らなければ効果的な監視はできない。ベンダーのサポートなどを利用して記録を分析することが望ましい。また技術力のあるベンダーかどうかで，同じツールでも効果は変わる。

(高橋 信頼=nob@nikkeibp.co.jp)

PEST AVAILABLE COPY

▶99年12月号の特集に引き続き，2000年もWANサービスの動向に注目したいと思います。アクセス回線では無線やADSLなどが選択肢として増えるほか，バックボーン系では，"次世代IP-VPNサービス"が登場します。これらが大幅に安く提供されるならば，企業のWANが劇的に変わるかもしれません。（榊原）

▶「Oracleがどう動くかをイメージしながらチューニングしている」。ある優秀なSEのコメントです。システムが思い通りに動かないとき，解決するためにはコンピュータがどう動いているかを想像する力が必要です。今月からの連載「プログラムが動く仕組み」のテーマは，この想像力です。（矢崎）

▶クリスマス商戦のさ中，米国出張してきました。TVコマーシャルや街頭広告に「.com（ドット・コム）」といったフレーズがさかんに見られたのには正直驚きました。

米国の小売業ではインターネットがすっかり浸透しているようです。ますます加熱するインターネット・ビジネスがこれからどうなるのか，海外の動きも積極的にレポートしていきたいと思います。（和田）

▶今月から特集Ⅱに代わり「注目技術・活用のポイント」と「注目製品・選択のポイント」という新コーナーを設けました。ご意見，ご感想をメール（replynos@nikkeibp.co.jpあて）でいただければ幸いです。本年もよろしくお願いいたします。（井上）

訂正

99年11月号特集Ⅱ「PostgreSQLの実力」，189ページの図Dにおいて，同期と非同期のグラフ・ラベルが入れ替わっていました。正しくは図の説明のとおり非同期モードの方が高速です。99年12月号「解説●2000年へ向けて高まるウイルスの脅威」127ページの表2でトレンドマイクロのURLがhttp://www.nai.com/japan/となっていますがこれはネットワーク アソシエイツのURLで，トレンドマイクロはhttp://www.trendmicro.co.jp/です。以上，おわびして訂正いたします。

日経オープンシステム ©日経BP社 2000 ISSN 0918-5992 ●本誌記事の無断転載を禁じます

読者の皆様へ
●本誌購読のお申し込み，住所・勤務先の変更は，日経BPお客さまセンターへ
〒134-8729 東京・江戸川郵便局 私書箱240号
☎(03)5696-1111（平日9:00～17:00）
●本誌の記事検索やダウンロードは，日経BPニュースサービスをご利用ください。
URL：http://bijiken.nikkeibp.co.jp/
●返本・欠本は本誌お取り替えいたします。ご近辺サービスセンターまでご連絡ください。
●日経BP社はインターネットのWWWサーバーで情報を発信しています。
ホームページのアドレス（URL）は，
http://www.nikkeibp.co.jp/です。

発行人●松島 聡
編集長●井上 望
副編集長●吉川 和宏／小原 聡
執筆●森脇 真一／高橋 信頼／森山 徹／松山 貴之／矢崎 茂則／神原 厚／福島 陽宏
広告担当●高田 良彦
広告部次長●加藤 敏　広告部副長●坂元 宏
広告●新村 尚徳／福岸 正夫／岸川 大輔／佐生 基
販売部次長●服部 昇
販売部副長●大西 茂樹
デザイン・制作●エステム
制作協力●日経BPクリエーティブ
写真●オリオンプレス／センシン企画
イラスト●深田 次郎

日経BP社
Nikkei Business Publications, Inc.
〒102-8622 東京都千代田区平河町2-7-6

日本ABC協会加盟誌（第三者機関認証公査部数）

受入 平成 12.1.14 ソフトウェア情報センター

Citation 2

プロジェクトベース グループウェア
ORQUESTA オルケスタ
こんな会社にオルケスタ
進捗の見積りを営業戦略に活かしたい
時間のロスを減らしたい
営業と工場の原価を正確に把握したい
プロジェクトを核に情報の共有
掲示板 スケジュール 経費管理 ToDoリスト 住所録 名刺自報 会議予約 プロジェクト内 工程表 日報一覧 会議室 売上一覧 ToDo一覧 進捗一覧
工程表画面
クライアント側に必要なものはWEBブラウザだけです。
ASPソースコードを公開しておりますので，自在にカスタマイズしてご利用いただけます。
ODBCデータベースを使用しておりますので，他システムとの連携も可能です。
対応サーバーOSはWindows NT Server およびWorkstation，Windows 2000（予定）。
デモサイトを用意しております。
VELTEC
株式会社ヴェルテック
〒151-0072 東京都渋谷区幡ヶ谷2-27-7
TEL.03-5365-2464 FAX.03-5365-2463
mail info@veltec.co.jp
http://www.veltec.co.jp
（資料請求番号321）



BEST AVAILABLE COPY